Leçon 107 : Congruences dans $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$ - Applications

Prérequis : arithmétique, div euclidienne

I) Congruences dans $\mathbb{Z}$

Propriété 1. *Soit $n \in \mathbb{N}$. La relation $\Re_n$ définie sur $\mathbb{Z}$ par :*
$x \Re_n y \Leftrightarrow x-y \in n\mathbb{Z}$ est une relation d'équivalence.

Définition 1. *Cette relation d'équivalence est appelée relation de congruence modulo n. On note $x \equiv y$ (mod n) pour $x \Re_n y$*

Propriété 2. *Soit $n \in \mathbb{N}$ et $n \geqslant 2$*
On a $x \equiv y$ (mod n) $\Leftrightarrow$ x et y ont le même reste dans la division euclidienne par n.

Remarques : 1) Tout $x \in \mathbb{Z}$ a un équivalent dans $\{0, 1, ..., n-1\}$ 2) 2 éléments distincts de $\{0, 1, ..., n-1\}$ ne sont pas équivalents.

Définition 2. *On dit que les éléments de $\{0, 1, ..., n-1\}$ sont les représentants canoniques des classes d'équivalence modulo n.*
On note l'ensemble des classes d'équivalence pour $\Re_n$ sous la forme $\mathbb{Z}/n\mathbb{Z}$

Propriété 3. *L'addition et la multiplication de $\mathbb{Z}$ sont compatibles avec la congruence modulo n.*

II) Anneau $\mathbb{Z}/n\mathbb{Z}$

1) généralités

Propriété 4. *On définit sur $\mathbb{Z}/n\mathbb{Z}$ des lois de composition internes en posant :*
$\forall (x, y) \in \mathbb{Z}^2$, $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x}.\overline{y} = \overline{x.y}$

Propriété 5. *$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.*
La surjection canonique de $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneau.

Exemple :
table d'addition et de multiplication de $\mathbb{Z}/4\mathbb{Z}$ et de $\mathbb{Z}/5\mathbb{Z}$

2) inversibles de $\mathbb{Z}/n\mathbb{Z}$

Propriété 6. *Soit $n \geqslant 2$ et $x \in \mathbb{N}$ $\overline{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi $x \wedge n = 1$*

Définition 3. *Soit $n \geqslant 2$*
On note $\varphi(n) = Card\{k \in \{0, 1, ..., n\} / k \wedge n = 1\}$
On l'appelle l'indicatrice d'Euler

Propriété 7. *Soit $(\mathbb{Z}/n\mathbb{Z})^\star$ l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$. C'est un groupe abélien de cardinal $\varphi(n)$*

Théorème 1. *Soit $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps ssi p est premier*

III) applications

1) th chinois

2) Th de Wilson

3) équations diophantiennes

4) Calculs de $\varphi(n)$

5)écriture décimale